International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

How Android Application Permissions Impact User's Data Privacy?

Shweta Shankar Wader

Student, Department of Information Technology, Keraleeya Samajam(REGD.) Dombivli's Model College, Maharashtra, India

ABSTRACT

Android is the most common OS(operating system) for mobile devices. There are approximately 2.7 million applications on the Google Play Store .There is a huge possibility that cyber criminals will try to exploit this situation. Android worksin terms of permissions, in order to secureuser's data from exploitation. This means that hardware and data can only be accessed only when apps are allowed i.e. when they are given permission. Android permissions are threatening to user's data privacy because, even though their main goal was to protect user's privacy, they can compromise the data stored on the device if they are granted to a malicious application. A lot of 'free' applications tend to request redundant permissions, often with the purpose to gather user's private and valuable data. This study mostly takes a note of how these application permissions can have an impact on the user's data privacy?

Keywords: Android, Application Permissions, Data Privacy

1. Introduction

Android has a permission restricted access model to provide access to confidential resources (e.g. sd card, contacts). This means that to realize access to those resources, apps should declare within the manifest the specified permissions, which users may grant or not. However, applications might abuse this model so as to realize access to non-public information. Typical examples are applications that ask for more permissions which aren't really required named as overprivileged (Felt et al., 2011). These applications are often silently transformed into malware whenever an OS or an app update occurs, using an attack that's called privilege escalation through updating.

The growing number of permissions from the first version of Android to the lasts version does not help to solve the security issues as it represents an increase in the Android attack surface. Furthermore, the bulk of users are still using previous versions that, differently from Android 6.0, doesn't foresee the likelihood of selectively deciding which subset of the requested permissions should be granted to an app. This issue, combined with the very fact that it's not very easy to know the meaning of every requested permission, since they're too many and not clearly documented, makes things very dangerous for users from a security and privacy point of view.

Research has shown that few users read the Android install-time permission requests and even fewer understand them them . Android doesn't offer any capability to users for dynamically enabling, modifying, and configuring the permissions. The only method available to users is to cancel the app permissions or non-revoke them from the device settings. The main drawback of Android Permission Architecture is that there's no technique that permits an App developer to acknowledge the foremost significant permissions needed by the app functionality. The developer will then request more privileged ones consistent with some check and stability criteria, which protect the privacy of the user. Thus, it results in have many malicious applications and other online services that negatively impact the reliability of user private resources, or they'll also affect the mobile device itself.

* *Corresponding author.*
E-mail address: shwetaw812@gmail.com

2. Background/Literature Review

The evolving state of recent mobile operating systems and therefore the proliferation of mobile services is more and more catching the eye of malicious users. Their main goal is to realize access to otherwise private information by exploiting vulnerabilities both at application and OS level. Many papers within the literature (Enck et al, 2010, Gibler et al, 2012, Stirparo, Kounelis, 2012, Zhou, Jiang, 2013) have shown apps with high invasion and manipulation on users' personal data.

The goal of Android's permissions model is to guard system resources from indiscriminate and unauthorised use by apps. However, this model has some inherent problems which may affect users privacy and anonymity also . The following paragraphs describe the kinds of threats we've identified which target this model, namely threats related to: pre-installed apps, permission management, permission granularity, permission notification, unused permissions, and lack of security.

First of all, pre-installed apps are by default granted all permissions required and are considered trusted since they're a part of the OS firmware. Therefore, users aren't informed about the specified permissions of those apps, since consent is generally granted by users during the installation process. This means that users don't have any indication on which resources are accessed by these apps and that they are susceptible to privacy invasive behaviours.

The second important point is that the way permissions are managed and granted during the app life-cycle. Consequently, a standard behaviour is simply to simply accept all the permission requests so as to succeed in the top of the installation process. Besides, most of the users don't have knowledge about possible risks the requested permissions introduce toward their personal data, and therefore the information prompted during the installation process are not really informative about the important functionalities the app goes to access and the way often (e.g., regular fine grain location tracking). More knowledgeable users might attempt to evaluate the list of requested permissions, but even for experts it's unclear how permissions are used (Felt et al., 2012).

Threats to users' privacy could also be posed not only by malware apps but also by legitimate apps. Many legitimate apps are characterised by a particular degree of privacy invasiveness, which is said to the permissions they request and to which use they create out of the protected methods. In this direction, TaintDroid (Enck et al., 2010) also as other research works (Gibler et al, 2012, Stirparo, Kounelis, 2012, Zhou, Jiang, 2013) demonstrate the sort of end-users' personal data manipulation performed by mobile apps. Examples of privacy invasive behaviour performed by apps are, as an example , games that request access to unique identifiers or user location that aren't needed by the app to function. Ultimately, it's up to every mobile device user to guage if an app behaviour is privacy-invasive consistent with his/her personal perceptions.

3. Method and Materials

Secondary quantitative research method was performed for this paper. Secondary research is a kind of research that involves using pre-existing data. Secondary research includes research articles published in research reports or journals as such . These documents are often made available on the net or offline by libraries, websites and so on. . Secondary research method involves re-analysing past data. Secondary research also includes :1. Online Data, 2. Data from Government and Non-government Archives, 3.Data from Libraries, 4. Data from Institutions of Learning.

Advantages of Secondary Research

- Easily Accessible
- Secondary research is cost-effective
- It is not time consuming
- It helps researchers to identify knowledge gaps which can be used as the basis of further systematic investigation.
- It is useful for scaling the scope of research & setting the stage for field investigations.

4. Data and Results

These are some dangerous permissions in the Android Developer’s Reference from Google. They are as follows

ACCEPT_HANDOVER

This permission allows for a call to be redirected to an app or a service . If you are unaware of it then this could end up costing you as it could be used to secretly record conversations.

ACCESS_FINE_LOCATION

This permission will take GPS and WiFi data to get your exact location. The accuracy could be possibly locating which room you’re in within your home.

ACCESS_MEDIA_LOCATION

Unless you’ve turned off geotagging on your pictures and videos, this app can build an accurate profile of where you’ve been based on data in your photo files.

ACTIVITY_RECOGNITION

Ifthis permission is put together with other location information and they can figure out what you’re doing and where you’re doing it.

ADD_VOICEMAIL

It is used in an application to add voicemails into the system.

This could be used for phishing purposes.

ANSWER_PHONE_CALLS

It gives access to an application to answer an incoming phone call.”

Imagine an app answering your phone calls and doing whatever it wants with the calls.

BODY_SENSORS

It gives access to an application to access data from sensors that the user uses to live what's happening inside their body, like pulse .”

This is another one where the knowledge on its own won't mean much, but when including information from other sensors could prove very revealing.

CALL_PHONE

It gives access to an application to initiate a call without browsing the Dialer interface for the user to verify the decision .”

It’s scary enough to think an app could make a call without you knowing it. Then believe how it'd call a 1-900 number and you'll get on the hook for hundreds or thousands of dollars.

READ_CALENDAR

It gives access to an application to read the user’s calendar data.”

The app would know where you’ll be and the exact data . Also, if you create notes with your appointments, it’ll also know the reason as to you’re there.

WRITE_CALENDAR

It gives access to an application to write the user’s calendar data.”

A bad actor might use this to place appointments in your calendar making you think that you would possibly need to go somewhere you don’t, or call someone you don’t got to .

READ_CALL_LOG

It gives access to an application to read the user’s call log.”

Who we ask and when are often very revealing about our lives. Calling your co-worker during the day? Normal. Calling them at 2 a.m. on Saturday night? Not so normal.

WRITE_CALL_LOG

It gives access to an application to write (but not read) the user’s call log data.”

It’s unlikely to happen, but a malicious app could add call logs to line you up for something.

READ_CONTACTS

It gives access to anapplication to read the user’s contacts data.”

Similar to reading the decision log, a person’s contact list says tons about them. Plus, the list could also be wont to phish your friends, making them think it’s you messaging them. It also can be wont to grow a marketing email list the corporate could then unload to advertisers.

WRITE_CONTACTS

It gives access to anapplication to write down the user’s contacts data.”

What if this might be wont to edit or overwrite your contacts? Imagine if it changed the amount for your mortgage broker to a different number and you call some scammer and provides them your financial information.

READ_EXTERNAL_STORAGE

It gives access to anapplication to read from external storage.

Any data storage that plugs into your devicecould be accessed if you allow this permission.

WRITE_EXTERNAL_STORAGE

It gives access to anapplication to write to external storage.

READ_PHONE_NUMBERS

It gives access to an application to read access to the device’s phone number(s).

READ_PHONE_STATE

It gives access to an application read only access to phone state, including the present cellular network information, the status of any ongoing calls, and an inventory of any phone accounts registered on the device.

It can be used to facilitate eavesdropping and tracking your location by which network you’re on.

READ_SMS

It gives access to an application to read SMS messages.”

A way to eavesdrop on the user and gather personal informationby reading your text messages.

SEND_SMS

It gives access to an application to send SMS messages and can cost you tons of cash , quickly.

RECEIVE_MMS

It gives access to an application to monitor incoming MMS messages.

The app would be ready to see any pictures or videos that were sent to you.

RECEIVE_SMS

It gives access to an application to receive SMS messages.

This app would leave monitoring your text messages.

RECEIVE_WAP_PUSH

It gives access to an application to receive WAP push messages.

A WAP push message may be a message that's also an internet link. It could open a phishing or malware laden internet site by choosing a message.

RECORD_AUDIO

It gives access to an application to record audio.
Yet another way to eavesdrop on people. Plus there’s a surprising amount you'll learn from the sounds around an individual , albeit they’re not talking.
USE_SIP
It gives access to an application to use SIP service.

5. Discussions

The apps you install may question you for the permission to access your contacts, location, microphone, phone, storage and sensors. Some permissions are required for the app to figure properly . If it's a mapping app, then location information becomes necessary. If it's a normal gaming asking for your location then just deny the access to it.

If you give apps access to your microphone, then there is a possibility that somebody can eavesdrop on the the device communications so be cautious while granting access to it.

Getting into the habit of scanning and reading your app permissions carefully will make you more aware of what apps are doing with your device.

Enable or disable app permissions one by one

If you put in an app with all permissions disabled, you'll still activate those you would like individually within the settings.

1. Go to Android phone's Settings app.
2. Tap on Apps or Application Manager.
3. Select the app that you simply want to vary by tapping Permissions.
4. Now choose which permissions to turn on or off, like camera or microphone.

• Scan for viruses and other flaws

1. Go to your Android phone's Settings app.
2. Tap Security.
3. Select Google Play Protect. From here, you will see all of the apps that are scanned and if any are suspect. If so, you'll be wanting to require steps to right away stop using those apps and obtain them off your phone.

• Google Play Protect scans all of your apps to recognise apps that can be harmful for user’s privacy.
• Turn off your location settings
• Turn off location data in your photos

6. Conclusion

The Android operating system supports users' privacy using apps permission technique that put restrictions on all apps with regard to accessing a user’s private data. Each app requires a list of permissions, which are determined by the app developer and accepted by the user during the app installation time. The ability to avoid granting dangerous permissions is delegated to the end-user, who is expected to understand what permissions have been accepted. Android does not provide tools to analyze and trace the possible interactions between apps. This work has analyzed the most popular Android apps and discussed numerous privacy concerns associated with the permission grants required by these

apps, especially within the context of communications and social media apps. The authors note that most of the mobile apps use over-privileges permissions and misuse users' private data. It is often unclear to end users how apps are accessing resources and personal information on their devices. Furthermore, most of these applications request over-privileges permissions, which cannot be handled by the user, although new versions of Android platform are available. Permission techniques are not effective enough to protect the user privacy, as they can be attacked in different ways e.g. Ads libraries, social networking ads and e-commerce channels. Therefore, providing users with a mechanism to trace, control and configure their data and privacy is very critical.

Suggestions :

Mobile applications benefits users by providing various services but it must not come at the expense of users’ data privacy rights.

The following are to be considered when using apps:

Read privacy notices. A privacy notice will give you information on how your data will be processed, the nature and extent of processing, your rights as data subjects and how you may exercise these rights.

Be cautiousregarding the info you provide: Provide data that is required for the app’s to function.

Take a note of your privacy settings and always keep checking it.

Check the permissions: Applications collect many permissions – permissions that aren't required for the applications to perform their functions. This may result in potential risks.

Limitations: Since this paper was based on secondary research it has its limitations like secondary data can be general and vague and may not really help companies with decision making.

Acknowledgements

I would like to express my special thanks of gratitude to all my teachers for their able guidance and support in completing my research

References

[1]https://www.cnet.com/how-to/over-1000-android-apps-were-found-to-steal-your-data-heres-what-you-can-do/
"Over 1,000 Android apps were found to steal your data. Here's what you can do Your privacy may be at stake, even if you deny these apps permission."By Katie Conner (July 16, 2019 7:00 a.m. PT)

[2]https://www.online-tech-tips.com/smartphones/30-app-permissions-to-avoid-on-android/ "30 App Permissions To Avoid On Android.
Don't give them too much access" by: Guy McDowell, Twitter: @GuyMcDowell
Posted on: October 1st, 2020 in: Smartphones

[3]https://www.researchgate.net/publication/332401070_Android_Application_Permission_Model_Issues_and_Privacy_Violation
"Android Application Permission Model Issues and Privacy Violation"April 2019 Conference: FREE AND OPEN SOURCE SOFTWARE CONFERENCE (FOSSC'2019-OMAN) At: Sultanate of Oman – Muscat Authors:Zainab Alkindi(Sultan Qaboos University),Mohamed Sarrab (Sultan Qaboos University) , Nasser Alzeidi (Sultan Qaboos University)

[4]https://www.researchgate.net/publication/322011457_Android_permission_system_and_user_privacy_- _A_review_of_concept_and_approaches "Android permission system and user privacy — A review of concept and approaches"
December 2017. Conference: 2017 IEEE 7th International Conference on Consumer Electronics - Berlin (ICCE-Berlin)
Project: Security and privacy for smartphones Authors:Asma K. (National University of Ireland, Galway) , Peter Corcoran (National University of Ireland, Galway)

[5]https://www.pewresearch.org/internet/2015/11/10/an-analysis-of-android-app-permissions/ NOVEMBER 10, 2015, "APPS PERMISSIONS IN THE GOOGLE PLAY STORE". Chapter 3: An Analysis of Android App Permissions
BY MICHELLE ATKINSON

[6]https://www.privacy.gov.ph/2020/02/managing-mobile-app-permissions/#:~:text=Mobile%20App%20Permission,access%20to%20a%20phone's%20hardware.&text=By%20downloading%20these%20applications%2C%20users%20unknowingly%20expose%20themselves%20to%20privacy%20risks.
Managing Mobile App Permissions February 14, 2020 | 6:01 PM GMT+0800 Last Edit: February 14, 2020

[7] https://developer.android.com/guide/topics/permissions/overview Permissions on Android

[8] https://appcare.co.in/how-does-app-permissions-impact-your-mobile-performance-what-kind-of-permissions-are-safe-to-allow-2/
How Does App Permissions Impact Your Mobile Performance? & What Kind Of Permissions Are Safe To Allow

[9]S. Jana and V. Shmatikov, 'Memento : Learning Secrets from Process Footprints', in IEEE symposium on security andprivacy., 2012, pp. 143–57.

[10]J. Gu, Y. Calvin, H. Xu, C. Zhang, and H. Ling, 'Privacylikelihood model perspective', Decis. Support Syst., vol. 94,pp. 19–28, 2017.

[11]B. Li, Y. Zhang, J. Li, W. Yang, and D. Gu, 'The Journal of Systems and Software AppSpear : Automating the hidden- code extraction and reassembling of packed android
malware', J. Syst. Softw., vol. 140, pp. 3–16, 2018.

[12] N. K. Thanigaivelan, A. Hakkala, S. Virtanen, and J. Isoaho, 'CoDRA : Context-based dynamically recon fi gurable access control system for android', vol. 101, no. April 2017, pp. 1– 17, 2018.

[13] C. Lyvas, C. Lambrinoudakis, and D. Geneiatakis, 'Dypermin : Dynamic permission mining', Comput. Secur., vol. 77, pp. 472–487, 2018.

[14] S. E. E. Profile, 'Malware Analysis and Detection on Android: The Big Challenge', in Smartphones from an Applied Research Perspective, no. November, 2017, pp. 198-211.

[15] A. Khatoon, G. S. Member, and P. Corcoran, 'Android permission system and user privacy- A review of concept and approaches', no. December, 2017.